PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-160855
(43)Date of publication of application : 21.06.1996

(51)Int.Cl. G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-298702
(22)Date of filing : 01.12.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TAKASHIMA YOICHI
ISHII SHINJI
YAMANAKA KIYOSHI

(54) DIGITAL INFORMATION PROTECTION SYSTEM AND ITS METHOD

(57)Abstract:
PURPOSE: To provide a digital information protection system and its method without information leaked to a third person and with the difficulty of illegal copying performed by a correct user.
CONSTITUTION: The information identifier of information to be utilized selected from an information terminal device 2 by a user is sent to a calculator card 3 and given a sign, this is transmitted to an information center 1, in the information center 1 a key WK is produced for ciphering the information to be utilized, this is stored in the calculator card 3 via the information terminal device 2, a WK request message including a random number (r) is sent from the information terminal device 2 to the calculator card 3, the stored key WK is set to the information terminal device 2 and the information to be utilized ciphered with the key WK and distributed from the information center 1 is decoded with the set key WK.

LEGAL STATUS

[Date of request for examination]	27.10.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3327435
[Date of registration]	12.07.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] The digital information protection system characterized by using said digital information with an information terminal unit, decoding with the secret decode key WK in the calculating-machine card which delivers the digital information enciphered with the public key of a common key encryption system or a public key cryptosystem from an information centre to an information terminal unit through a communication line, wireless, package media, etc., and is distributed from the information centre in advance.

[Claim 2] An information centre is a digital-information protection system according to claim 1 characterized by to provide an information storage means to accumulate digital information, a communications control means to perform the communication link with an information terminal unit, a key generation means to generate an information cryptographic key and a decode key, an encryption means to encipher digital information, the public-key-encryption-ized means for carrying out cryptocommunication of the key, and the signature (public-key-

encryption decode) conversion means for signing.
[Claim 3] A communications control means by which an information terminal unit performs the communication link with an information centre, and a communications control means to perform the communication link with a computer card, An information storage means to accumulate digital information, and the public-key-encryption-ized means for carrying out cryptocommunication of the key, The signature (public-key-encryption decode) conversion means for signing, and a random-number-generation means to generate a random number, A collating means to collate the value of said random number and the random number received from the computer card, A private key are recording means to store the private key of self-equipment, and a decode means to decode key information and digital information, The digital information protection system according to claim 1 characterized by providing a security means to protect physically the secrecy of said random-number-generation means, a collating means, a private key are recording means, and a decode means.
[Claim 4] A computer card is a digital information protection system according to claim 1 characterized by providing a communications control means to perform the communication link with an information terminal unit, the public-key-encryption-ized means for carrying out cryptocommunication of the key, the signature (public-key-encryption decode) conversion means for signing, and a decode key are recording means to store the decode key WK.
[Claim 5] The digital information protection system according to claim 1 characterized by having an information centre according to claim 2, an information terminal unit according to claim 3, and a calculating-machine card according to claim 4.
[Claim 6] A computer card and an information terminal unit attest mutually, and a computer card checks a user. Sign a user's demand information, encipher further and an information centre is accessed. Carry out cryptocommunication of the key WK for enciphering use information by the public key cryptosystem, and it registers with a computer card before information use. Transmit the receipt signature of Key WK to an information centre, and WK demand message sent automatically is received from an information terminal unit. Decoding with an information terminal unit, if Key WK is set in an information terminal unit and the encryption information from an information centre is sent to an information terminal unit by sending the encryption information on the key WK which changes each time using the random number in it to an information terminal unit The digital information protection approach characterized by to use the information on-line and

recording demand information, the receipt signature of Key WK, and the receipt signature of encryption information as an accounting basis.
[Claim 7] The digital information protection approach according to claim 6 characterized by confirming whether the information terminal unit has reception, and an original random number and original consistency in that to which delivery and a computer card carried out signature encryption of the random number which the information terminal unit generated at the computer card as an approach which a computer card and an information terminal unit attest mutually.
[Claim 8] It is the digital-information protection approach according to claim 6 characterized by to control to store in the computer card the password defined beforehand as an approach a computer card attests the user who operates an information terminal unit , to confirm that the character string inputted from the information terminal unit is in agreement , to carry out error processing when an input error exceeds a predetermined count , and to repeal a computer card when this error is repeated continuously the fixed number of times .
[Claim 9] As an approach a computer card attests the user who operates an information terminal unit The password defined beforehand is enciphered and stored in the computer card. The character string inputted from the information terminal unit The digital information protection approach according to claim 6 characterized by confirming whether it is in agreement with what was enciphered (or is what decoded the enciphered password which was stored in the computer card in agreement with what was inputted from the information terminal unit or not?).
[Claim 10] As an approach a computer card attests the user who operates an information terminal unit Encipher the password defined beforehand on a computer card, or it stores as it is. Cryptocommunication of the character string inputted from the information terminal unit is carried out between an information terminal unit and a computer card. The digital information protection approach according to claim 6 characterized by adjusting the parity of the random number which confirmed whether it would be in agreement with the thing or the thing as it is which the inputted character string enciphered, and was generated by whether it is in agreement, and carrying out cryptocommunication of the random number.
[Claim 11] As an approach a computer card attests the user who operates an information terminal unit Encipher the password defined beforehand on a computer card, or it stores as it is. The random number generated with the information terminal unit is added to the character string inputted

from the information terminal unit (or an exclusive OR -- taking). The password beforehand registered from the character string which carried out cryptocommunication between the information terminal unit and the computer card, and has been sent with the computer card is lengthened (or an exclusive OR -- taking). The digital information protection approach according to claim 6 characterized by checking by whether the random number which returned the acquired value to the information terminal unit and was generated with the information terminal unit, and the returned value are in agreement.

[Claim 12] The digital information protection approach according to claim 6 characterized by preventing unlawful access to an information centre when the informational information identifier and the public key of an information centre which the user chose, and its certificate are transmitted to a computer card, and a computer card carries out signature encryption at an information identifier, adds the public key and certificate of a computer card to it with an information terminal unit and transmits to an information centre.

[Claim 13] An information centre generates the key WK for enciphering use information, and it enciphers with the public key of a computer card. The signature of an information centre is attached to it and an information terminal unit is minded. To a computer card Delivery, The digital information protection approach according to claim 6 characterized by the signature verifying whether it is the right with a computer card, obtaining Key WK, transmitting the receipt signature of this key WK to an information centre through an information terminal unit, and accumulating Key WK with an information identifier as it is not read unjustly.

[Claim 14] The digital information protection approach according to claim 6 characterized by transmitting WK demand message containing a random number r into a calculating-machine card after an information terminal unit sends out the receipt signature of Key WK to an information centre.

[Claim 15] The digital information protection approach according to claim 6 characterized by decoding the encryption information which confirms whether a random number is in agreement, sets Key WK, and is sent from an information centre after combining the random number and WK in WK demand message with a calculating-machine card, enciphering with the public key of an information terminal unit, transmitting to an information terminal unit and decoding it with an information terminal unit.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the digital information protection system which can prevent the unjust duplicate of digital information, such as music, an image, and a program, and its approach.
[0002]
[Description of the Prior Art] Works, such as music, an image, pictures, and books, are changed into digital information, compression coding is carried out, and development of the high-speed digital communication technique which makes representation digital information compression technology (for example, MPEG=Moving Picture Experts Group, JPEG=Joint Photographic Coding Experts Group, etc.) and ISDN, such as voice, an animation, and a still picture, in recent years has enabled it to deliver from an information centre etc. to each user terminal through a communication line.
[0003] There is an example which has already carried out distribution service about computer software with little amount of data using personal computer communications etc. compared with digital information, such as an image mentioned above. moreover, recently by the sales method of the computer software by CD-ROM by which service was started in the U.S. If the user who sold and distributed CD-ROM which stored the enciphered software for sale and the software for a demonstration which is not enciphered by the low price, and tried the software for a demonstration applies for purchase hope to a service center by telephone etc. The format which enables use of the software for sale which notified this user of the decode key and was enciphered is taken.
[0004]
[Problem(s) to be Solved by the Invention] In the case of the sales method of the software by the conventional personal computer communications mentioned above, encryption of software was not made but there was a problem of offering the environment where an illegal copy is made easier, compared with the sales method of the software by packages, such as a floppy disk.
[0005] Moreover, since in the case of the sales method of the software

by CD-ROM mentioned above center operation was intervened in case a decode key is received from a service center by telephone etc., the help started and there was a problem that a user's privacy could not be maintained. Moreover, since a help was minded, there was a problem that an illegal copy became possible according to injustice, such as sale through illegal channels of a decode key.

[0006] Without information leaking to the 3rd person, even if the purpose of this invention is a right user, an illegal copy is to offer a difficult digital information protection system and its approach.

[0007]

[Means for Solving the Problem] In this invention, in order to attain said purpose, the equipment in which it was sealed physically is put into an information terminal unit, and the key WK for decoding is accumulated in a computer card, and it is characterized by an information centre recording demand information, a key receipt signature, and an information receipt signature as a used proof.

[0008]

[Function] It becomes the system about which an information provider since the illegal copy is difficult in order for the equipment which it is difficult for there to be no possibility that information may leak to the 3rd person since according to this invention information is enciphered and it is delivering, and to shut up the decode key into the computer card, and to get to know a decode key even by the right user, and has been physically sealed to an information terminal unit to perform decode of decode of Key WK and information feels easy and which he can use.

[0009]

[Example] Drawing 1 shows one example of the digital information protection system of this invention, and, for one, as for an information terminal unit and 3, an information centre and 2 are [a computer card and 4] authentication centers among drawing.

[0010] The information centre 1 accumulated the digital information of a large number supplied by the information provider, and has managed this like a database.

[0011] The information terminal unit 2 possesses the image display device for using digital information, an audio output device, etc., and is arranged at each user's home etc. Through the communication network, the information centre 1 and the information terminal unit 2 are connected so that two-way communication may be possible.

[0012] The computer card 3 is attached free [attachment and detachment] to the information terminal unit 2, and can store the data

in which the contents of dealings which information to have purchased are shown in the interior. This computer card 3 can be possessed for every user, and by connecting this computer card 3 to the information terminal unit 2, from an information centre 1, each user can make digital information [finishing / purchase] (an image, music, etc.) able to send to the information terminal unit 2, and can use it.
[0013] In addition, the authentication center 4 is needed only in the preparation phase at the time of using a public key cryptosystem.
[0014] Drawing 2 is what shows the detailed configuration of an information centre. (Configuration of an information centre) The information input section into which 11 input use information among drawing, the information storage section in which 12 accumulates use information, WK generation section which generates the key WK used when the information encryption section as which 13 enciphers use information, and 14 encipher use information, A signature transducer for the open transducer as which 15 enciphers Key WK, and the key WK with which 16 was enciphered to show that it is the thing of an information centre, Memory for 17 to memorize a result etc. in the middle of the certificate by the public key and its authentication center of an information centre, or an operation, CPU to which 18 performs control of the whole information centre and a hash algorithm, the public key verification section in which 19 verifies the public key of a computer card etc., and 20 are the network I/O sections which perform the exchange with a network.
[0015] Drawing 3 is what shows the detailed configuration of an information terminal unit. (Configuration of an information terminal unit) The card I/O section in which 21 perform the exchange with the computer card 3 among drawing, the decode key extract section in which 22 decodes public key encryption, The information decode section in which 23 decodes use information, the information output section which outputs the information by which 24 was decoded, A security means by which an image display device and 25b protect an audio output device, and, as for 25a, 26 protects physically the secrecy of the decode key extract section 22, the information decode section 23, and the information output section 24, The information storage section accumulated while 27 had had use information enciphered, the network I/O section in which 28 performs the exchange with a network, Memory for 29 to memorize a result etc. in the middle of the public key of an information terminal unit, the certificate of an authentication center, or an operation and 30 are CPUs which perform control and random-number generation of the whole information terminal unit, and a hash algorithm.

[0016] Drawing 4 is what shows the detailed configuration of a computer card. (Configuration of a computer card) The public key verification equipment to which, as for 31, a public key verifies a just thing with the certificate of an authentication center among drawing, The public-key-encryption equipment with which 32 performs encryption and signature conversion, the communication device with which 33 performs the communication link with the information terminal unit 2, The password collating unit with which 34 performs password collating for user authentication, The decode key registration equipment with which 35 registers the decode key of purchase information, the memory 36 remembers a result to be in the middle of the public key, certificate, and operation of a computer card, Electrical-potential-difference supervisory equipment required in order that CPU to which 37 performs control, random-number generation, etc. of the whole computer card, and 38 may hold the information on a private key etc., and 39 are the cells for backup.

[0017] (Information use protocol)

It expresses with M=DK (C) expressing with C=EK (M) the conversion which enciphers the <prior preparation> information M with Key K, and acquires the encryption information C, and decoding it. When using especially a public key cryptosystem, encryption is expressed with C=EKP (M), and it expresses decode with M=DKS (C). The latter may be used also as signature conversion.

[0018] Identifier IDU, a public key KPU, its certificate XPU, the public key KPC of the authentication center 4, and the private key KSU are beforehand written in the computer card 3, and especially the private key KSU is written in the area protected so that it could not read. In the authentication center 4, Certificate XPU has a public key KPU attested, and is called for as XPU=DKSC (XPU). However, KSC is the private key of the authentication center 4, and this is made secret in addition to authentication center 4.

[0019] Similarly, Identifier IDS, a public key KPS, its certificate XPS, the public key KPC of the authentication center 4, and a private key KSS are beforehand written in the information terminal unit 2, and Identifier IDM, a public key KPM, its certificate XPM, the public key KPC of the authentication center 4, and a private key KSM are beforehand written in an information centre 1. Moreover, it registers with the computer card 3 so that the information (for example, password) for attesting a user may not be read.

[0020] A computer card and <information terminal mutual recognition> drawing 5 show the process of a computer card and information terminal

mutual recognition.
[0021] If the computer card 3 is connected to the information terminal unit 2, the random number R, the public key KPS and the certificate XPS of a public key of this information terminal unit 2, and the identifier IDS of this information terminal unit 2 will be sent to the computer card 3 from the information terminal unit 2.
[0022] It judges whether the public key KPS of the information terminal unit 2 is just by checking whether the computer card 3 has the consistency of the public key KPS and Certificate XPS of the information terminal unit 2 using the public key KPC of the authentication center 4 currently held to the interior. the random number R sent when it is judged that it is just -- signature encryption conversion -- giving -- T=EKPS (DKSU (R)) (or DKSU (EKPS (R))) -- T, the public key KPU and Certificate XPU of the computer card 3, and Identifier IDU are transmitted to the information terminal unit 2.
[0023] A partner judges whether it is the right computer card IDU by checking whether the information terminal unit 2 has the consistency of sent T and sent R, after checking that the public key KPU of the computer card 3 is just using the public key KPC of the authentication center 4 currently held to the interior.
[0024] <User authentication> drawing 6 shows the process of user authentication.
[0025] A user enters into the information terminal unit 2 the password beforehand registered into the computer card 3. The information terminal unit 2 transmits the entered password to the computer card 3, and has it judged whether it is the right. The input of a password judges that he is a just user to a right case, and shows a user menu information.
[0026] Under the present circumstances, the input error of a password is permitted to the predetermined count appointed beforehand, for example, 3 times, it discharges the computer card 3 noting that it may not be error processing, i.e., a just user, when 3 times is exceeded, and it makes this card an invalid noting that it is not the fixed count which this error appointed beforehand further, for example, a user just when repeated 5 times in succession.
[0027] In addition, the password defined beforehand is enciphered and stored in the computer card as an option of user authentication. How to confirm whether it is in agreement with what the character string inputted from the information terminal unit enciphered (or is what decoded the enciphered password which was stored in the computer card in agreement with what was inputted from the information terminal unit or not?), Encipher the password defined beforehand on a computer card, or

it stores as it is. Cryptocommunication of the character string inputted from the information terminal unit is carried out between an information terminal unit and a computer card. It is confirmed whether it is in agreement with the thing or the thing as it is which the inputted character string enciphered. How to adjust the parity of the random number generated by whether it is in agreement, and carry out cryptocommunication of the random number, Encipher the password defined beforehand on a computer card, or it stores as it is. The random number generated with the information terminal unit is added to the character string inputted from the information terminal unit (or an exclusive OR -- taking). The password beforehand registered from the character string which carried out cryptocommunication between the information terminal unit and the computer card, and has been sent with the computer card is lengthened (or an exclusive OR -- taking). The acquired value is returned to an information terminal unit and the approach of checking by whether the random number generated with the information terminal unit and the returned value are in agreement etc. can be applied.

[0028] <User selection> drawing 7 shows the process of user selection, and a user chooses required information from menu information.

[0029] <Information-requirements> drawing 8 shows the process of information requirements of requiring information.

[0030] A user transmits the informational selected information identifier Req(s) (number which can specify as a meaning the information which whole-world common codes, such as an international recording code (ISRC), and an information provider gave uniquely in the case of music information) and the selected public key KPM of an information centre 1, and its certificate XPM to the computer card 3.

[0031] the computer card 3 has the consistency of the public key KPM and Certificate XPM of an information centre 1 with the public key KPC of the authentication center 4 -- checking -- Req -- signature encryption -- carrying out -- RU=EKPM (DKSU (Req)) -- RU is transmitted to the information terminal unit 2.

[0032] If RU is received, the information terminal unit 2 will add the public key KPU and Certificate XPU of the computer card 3 to it, and will transmit them to an information centre 1.

[0033] It checks that the information centre 1 has the consistency of the public key KPU and Certificate XPU of the sent computer card 3, Req is calculated as Req=EKPU (DKSM (RU)) from RU, and information is retrieved.

[0034] Key delivery and <key receipt signature> drawing 9 show the process of key delivery and a key receipt signature.

[0035] An information centre 1 generates the key WK for enciphering use information, and SKM and CK which SKM=DKSM (CK) Come to sign to CK which it CK=EKPU (WK) Comes to encipher with the public key KPU of the computer card 3 are transmitted to the computer card 3 via the information terminal unit 2.
[0036] the signature verifies whether it is the right and the computer card 3 decodes CK -- Key WK -- obtaining -- as the receipt signature of Key WK -- SU=DKSU (SKM) -- SU is transmitted to an information centre 1 via the information terminal unit 2. As Key WK is not read unjustly, it is accumulated with an information identifier.
[0037] <Key WK demand> drawing 10 shows the process of a key WK demand.
[0038] The information terminal unit 2 transmits WK demand message ReqW containing a random number r to the calculating-machine card 3, after sending out SU to an information centre 1.
[0039] Information delivery and <information use> drawing 11 show the process of information delivery and information use.
[0040] the computer card 3 -- the random number r and Key WK in ReqW -- joining together -- the public key KPS of the information terminal unit 2 -- enciphering -- V=EKPS (WK, r) -- V is transmitted to the information terminal unit 2. In the information terminal unit 2, after decoding V using KSS, it confirms whether r is in agreement and Key WK is set.
[0041] if an information centre 1, on the other hand, receives the key receipt signature SU -- Information I -- a batch -- dividing -- every unit of the -- said key WK -- enciphering -- C=EWK (I) -- C -- Hash Function h() -- giving -- signing -- SIM=DKSM (h (C)) -- SIM and C are sent to the information terminal unit 2. In the information terminal unit 2, the signature verifies the right thing and decodes the encryption information C.
[0042] In addition, the security protection is physically made to the equipment decoded by WK from the equipment decoded using KSS. It seals by putting an applicable part into a strong container as the implementation approach, or is R. Mori and
M. Kawahara' Superdistribution. : It is possible to apply the approach indicated by The Concept and theArchitecture' Trans. IEICE, E-73, No. 7, and 1990-7.
[0043] If C is decoded, the information terminal unit 2 is signed to it, and ACK=DKSS (h (C)) is returned to an information centre 1. After checking that an information centre 1 has just ACK, RU, SU, and ACK are recorded as an accounting basis. It checks that ACK comes back and processing is continued about the following batch.

[0044] In addition, although said example showed the case where public communication channels, such as ISDN, were used, it cannot be overemphasized that it is applicable also to connectionless circuits, such as a dedicated line.

[0045]

[Effect of the Invention] By separating the information body and decode key which were enciphered according to this invention, as explained above, and storing a decode key in insurance in a computer card From that information does not leak to the 3rd person, and an illegal copy being difficult Can constitute the system which an information provider can use in comfort, and, moreover, it does not become disadvantageous for a user. there is no information to use in a nearby information terminal unit -- ** -- it can use by accessing to an information centre, and there is an advantage, such as becoming available from every information terminal unit.

[0046] In addition, it cannot be overemphasized that this invention is applicable in the case of delivery by communication link use of not only computer software but all encryption digital information.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing showing one example of the digital information protection system of this invention

[Drawing 2] The detailed block diagram of an information centre

[Drawing 3] The detailed block diagram of an information terminal unit

[Drawing 4] The detailed block diagram of a computer card

[Drawing 5] Drawing showing the process of a computer card and information terminal mutual recognition

[Drawing 6] Drawing showing the process of user authentication

[Drawing 7] Drawing showing the process of user selection

[Drawing 8] Drawing showing the process of information requirements of requiring information

[Drawing 9] Drawing showing the process of key delivery and a key receipt signature

[Drawing 10] Drawing showing the process of a key WK demand

[Drawing 11] Drawing showing the process of information delivery and information use

[Description of Notations]
1 [-- Information input section,] -- An information centre, 2 -- An information terminal unit, 3 -- A computer card, 11 12 [-- A open transducer,] -- The information storage section, 13 -- The information encryption section, 14 -- WK generation section, 15 16 [-- Public key verification section,] -- A signature transducer, 17 -- Memory, 18 -- CPU, 19 20 -- The network I/O section, 21 -- The card I/O section, 22 -- Decode key extract section, 23 [-- Audio output device,] -- The information decode section, 24 -- The information output section, 25a -- An image display device, 25b 26 -- A security means, 27 -- The information storage section, 28 -- Network I/O section, 29 [-- Public-key-encryption equipment, 33 / -- A communication device, 34 / -- A password collating unit, 35 / -- Decode key registration equipment, 36 / -- Memory, 37 / -- CPU, 38 / -- Electrical-potential-difference supervisory equipment, 39 / -- Cell.] -- Memory, 30 -- CPU, 31 -- Public key verification equipment, 32